在 OCI 上部署 Threat Defense Virtual

您可以在 Oracle Cloud 基础设施 (OCI) 上部署 threat defense virtual，前者是一种公共云计算服务，使您能够在 Oracle 提供的高可用性托管环境中运行应用程序。

以下程序介绍了如何准备 OCI 环境并启动 threat defense virtual实例。您可以登录 OCI 门户，在 OCI 市场中搜索 Cisco Firepower NGFW 虚拟防火墙 (NGFWv) 产品，然后启动计算实例。启动 threat defense virtual后，您必须配置路由表，以便根据流量的源和目标将流量定向到防火墙。

- 概述， 第 2 页
- 端到端程序， 第 3 页
- 前提条件， 第 5 页
- 准则和限制， 第 5 页
- 网络拓扑示例， 第 7 页
- 如何管理 Cisco Secure Firewall Threat Defense Virtual 设备， 第 8 页
- 配置 OCI 环境， 第 9 页
- 在 OCI 上部署 Threat Defense Virtual， 第 13 页
- 连接接口， 第 14 页
- 为连接的 VNIC 添加路由规则， 第 15 页
- 部署 Auto Scale 解决方案， 第 16 页
- 前提条件， 第 17 页
- 加密密码， 第 24 页
- 准备 threat defense virtual 配置文件， 第 26 页
- 部署 Auto Scale 解决方案， 第 31 页
- 验证部署， 第 36 页
- 升级， 第 37 页
- 负载均衡器后端集， 第 37 页
- 从 OCI 中删除 Autoscale 配置， 第 38 页
- 使用 SSH 连接到 Threat Defense Virtual实例， 第 41 页
- 使用 OpenSSH 连接到 Threat Defense Virtual实例， 第 41 页
- 使用 PuTTY 连接到 Threat Defense Virtual实例， 第 42 页
- IPv6 故障排除， 第 43 页

概述

Cisco Cisco Secure Firewall Threat Defense Virtual 运行与物理 Cisco 威胁防御 相同的软件，以虚拟形式提供成熟的安全功能。threat defense virtual 可以部署在公共 OCI 中。然后，可以对其进行配置，以保护在一段时间内扩展、收缩或转换其位置的虚拟和物理数据中心工作负载。

OCI 计算资源大小

形状是确定分配给实例的 CPU 数量、内存量和其他资源的模板。threat defense virtual 支持以下 OCI 形状类型：

表 *1: Threat Defense Virtual* 支持的计算资源大小

OCI 形状	支持的 Threat Defense Virtual 版本	属性		接口
		oCPU	随机存取存储器 (GB)	
Intel VM.DenseIO2.8	7.3.x 及更高版本	8	120	最小值 4，最大值 8
Intel VM.StandardB1.4	7.3.x 及更高版本	4	48	最小值 4，最大值 4
Intel VM.StandardB1.8	7.3.x 及更高版本	4	96	最小值 4，最大值 8
Intel VM.Standard1.4	7.3.x 及更高版本	4	28	最小值 4，最大值 4
Intel VM.Standard1.8	7.3.x 及更高版本	8	56	最小值 4，最大值 8
Intel VM.Standard2.4	7.1、7.2.x 和 7.3.x	4	60	最小值 4，最大值 4
Intel VM.Standard2.8	7.1、7.2.x 和 7.3.x	8	120	最小值 4，最大值 8
Intel VM.Standard3.Flex*	7.3.x 及更高版本	4	16	最小值 4，最大值 4
	7.3.x 及更高版本	6	24	最小值 4，最大值 6
	7.3.x 及更高版本	8	32	最小值 4，最大值 8

OCI 形状	支持的 Threat Defense Virtual 版本	属性		接口
		oCPU	随机存取存储器 (GB)	
Intel VM.Optimized3.Flex*	7.3.x 及更高版本	4	16	最小值 4，最大值 8
	7.3.x 及更高版本	6	24	最小值 4，最大值 10
	7.3.x 及更高版本	8	32	最小值 4，最大值 10
AMD VM.Standard.E4.Flex*	7.3.x 及更高版本	4	16	最小值 4，最大值 4
	7.3.x 及更高版本	6	24	最小值 4，最大值 6
	7.3.x 及更高版本	8	32	最小值 4，最大值 8

- *7.4.x 及更高版本中的 Flex 形状支持 SR-IOV 模式。
- 在 OCI 中，1 个 oCPU 等于 2 个 vCPU。
- threat defense virtual 至少需要 4 个接口。

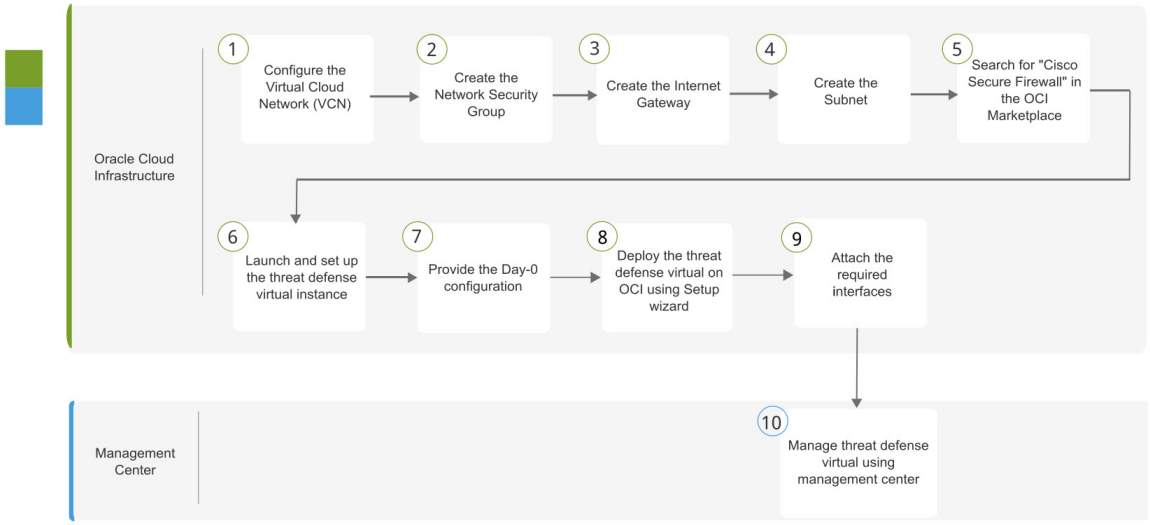
有关使用 Threat Defense Virtual 7.3 及更高版本支持的 OCI 计算形状的建议。

- OCI 市场映像版本 **7.3.0-69-v2** 及更高版本仅与 Threat Defense Virtual 7.3 及更高版本的 OCI 计算形状兼容。
- 您只能将 Threat Defense Virtual 7.3 及更高版本支持的 OCI 计算形状用于新部署。
- OCI 计算配置版本 **7.3.0-69-v3** 及更高版本与使用 Threat Defense Virtual 7.3 之前的 OCI 计算配置版本升级与 Threat Defense Virtual 一起部署的虚拟机不兼容。
- **VM.DenseIO2.8** 计算形态订用将继续计费，即使在您关闭实例后也是如此。有关详细信息，请参阅 OCI 文档。

您可以在 OCI 上创建账户，使用 Oracle 云市场上的思科 Firepower NGFW 虚拟防火墙（NGFWv）产品来启动计算实例，然后选择 OCI 形状。

端到端程序

以下流程图说明了在 Oracle Cloud 基础设施上部署 Threat Defense Virtual 的工作流程。



	工作空间	步骤
1	Oracle Cloud 基础设施	配置 OCI 环境：配置虚拟云网络 (VCN)（**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **CIDR 块 (CIDR block)** > **创建 VCN (Create VCN)**。
2	Oracle Cloud 基础设施	创建网络安全组：创建网络安全组。依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **网络安全组 (Network Security Groups)**，然后点击**创建网络安全组 (Create Network Security Group)**。
3	Oracle Cloud 基础设施	创建互联网网关：创建互联网网关。**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **互联网网关 (Internet Gateways)** > **创建互联网网关 (Create Internet Gateway)**。
4	Oracle Cloud 基础设施	创建子网：创建子网。**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **子网 (Subnets)** > **创建子网 (Create Subnet)**。
5	Oracle Cloud 基础设施	在 OCI 上部署 Threat Defense Virtual，第 13 页：在 OCI 市场中搜索“Cisco Secure Firewall”。
6	Oracle Cloud 基础设施	在 OCI 上部署 Threat Defense Virtual，第 13 页：启动并设置 Threat Defense Virtual 实例。
7	Oracle Cloud 基础设施	在 OCI 上部署 Threat Defense Virtual，第 13 页：提供 Day-0 配置。
8	Oracle Cloud 基础设施	在 OCI 上部署 Threat Defense Virtual，第 13 页：使用设置向导在 OCI 上部署 Threat Defense Virtual。

	工作空间	步骤
9	Oracle Cloud 基础设施	连接接口：连接接口。**计算 (Compute)** > **实例 (Instances)** > **实例详细信息 (Instance Details)** > **连接的 VNIC (Attached VNICs)**。
10	管理中心	使用管理中心管理 threat defense virtual

前提条件

- 在 https://www.oracle.com/cloud/ 上创建一个 OCI 账户。
- 思科智能账户。可以在思科软件中心 (https://software.cisco.com/) 创建一个账户。
- 许可 threat defense virtual。
  - 所有安全服务的许可证授权均在 管理中心中配置。
  - 有关如何管理许可证的详细信息，请参阅《*Cisco Secure Firewall Management Center* 管理员指南》中的“许可”。

注释 思科提供的所有默认许可证授权（以前用于 Firewall Threat Defense Virtual 虚拟设备）都将支持 IPv6 配置。

- 接口要求：
  - 管理接口 (2) - 一个用于将 threat defense virtual 连接到 管理中心，另一个用于诊断；无法用于直通流量。
  - 流量接口 (2) - 用于将 threat defense virtual 连接到内部主机和公共网络。
- 通信路径：
  - 用于访问 threat defense virtual的公共 IP。
- 有关 threat defense virtual 系统要求，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》。

准则和限制

支持的功能

- 在 OCI 虚拟云网络 (VCN) 中部署
- 路由模式（默认）

- 许可 - 仅支持 BYOL
- IPv6
- 仅 管理中心 支持。
- 支持单根 I/O 虚拟化 (SR-IOV)。

FTDv 智能许可的性能级别

threat defense virtual 支持性能层许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。

表 *2:* 基于授权的 ***Threat Defense Virtual*** 许可功能限制

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv5，100Mbps	4 核/8 GB	100Mbps	50
FTDv10，1Gbps	4 核/8 GB	1Gbps	250
FTDv20，3Gbps	4 核/8 GB	3 Gbps	250
FTDv30，5Gbps	8 核/16 GB	5Gbps	250
FTDv50，10Gbps	12 核/24 GB	10Gbps	750
FTDv100，16Gbps	16 核/32 GB	16Gbps	10,000

请参阅《*Cisco Secure Firewall Management Center* 管理员指南》中的“许可”一章，了解在许可 threat defense virtual 设备时的准则。

注释 要更改 vCPU/内存值，必须先关闭 threat defense virtual 设备的电源。

性能优化

为实现 threat defense virtual的最佳性能，您可以对 VM 和主机进行调整。有关详细信息，请参阅 OCI 上的虚拟化调整和优化。

接收端扩展 - threat defense virtual 支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量分发给多个处理器内核。在 7.0 及更高版本上受支持。有关详细信息，请参阅用于接收端扩展 (RSS) 的多个 RX 队列。

Snort

- 如果您观察到异常行为，例如 Snort 需要很长时间才能关闭，或者 VM 通常缓慢，或者在执行某个进程时，请从 threat defense virtual 和 VM 主机收集日志。收集总体 CPU 使用情况、内存、I/O 使用情况和读/写速度日志将有助于对问题进行故障排除。

- 当 Snort 关闭时，观察到高 CPU 和 I/O 使用率。如果在内存不足且没有专用 CPU 的单个主机上创建了大量 threat defense virtual 实例，则 Snort 将需要很长时间才能关闭，这将导致创建 Snort 核心。

不支持的功能

- 通过 设备管理器 提供本地管理支持。
- Threat Defense Virtual 本地 HA
- 透明/内联/被动模式
- 通过 DHCP 配置数据接口

限制

- OCI 上的 Threat Defense Virtual部署不支持将 Mellanox 5 作为 SR-IOV 模式下的 vNIC。
- IPv6 仅适用于根据 OCI 标准（VCN IPv4 和 IPv6）配置的　双堆栈。
- Firewall Threat Defense Virtual（ASAv 静态和 DHCP 配置）所需的单独路由规则。

网络拓扑示例

下图显示了在路由防火墙模式下建议用于 threat defense virtual 的拓扑，在 OCI 中为 threat defense virtual 配置了 4 个子网（管理、诊断、内部和外部）。

图 *1:* 包含四个 *VCN* 中的子网的 *OCI* 部署示例 *Threat Defense Virtual*

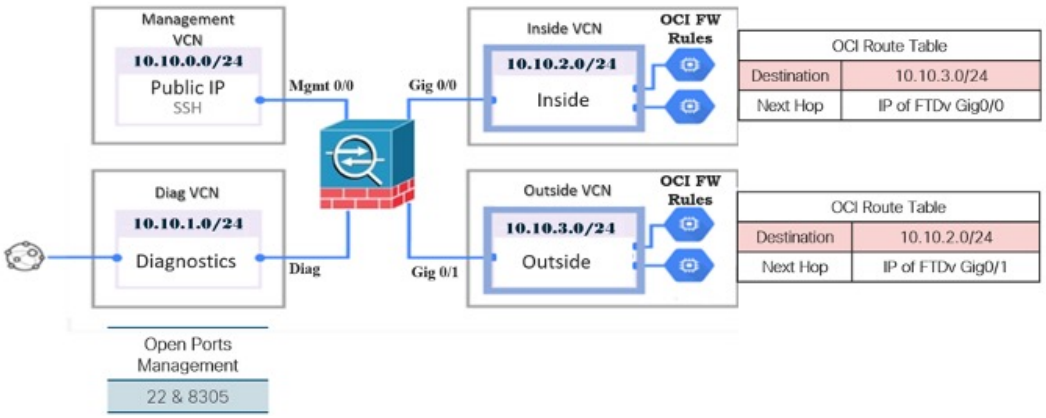
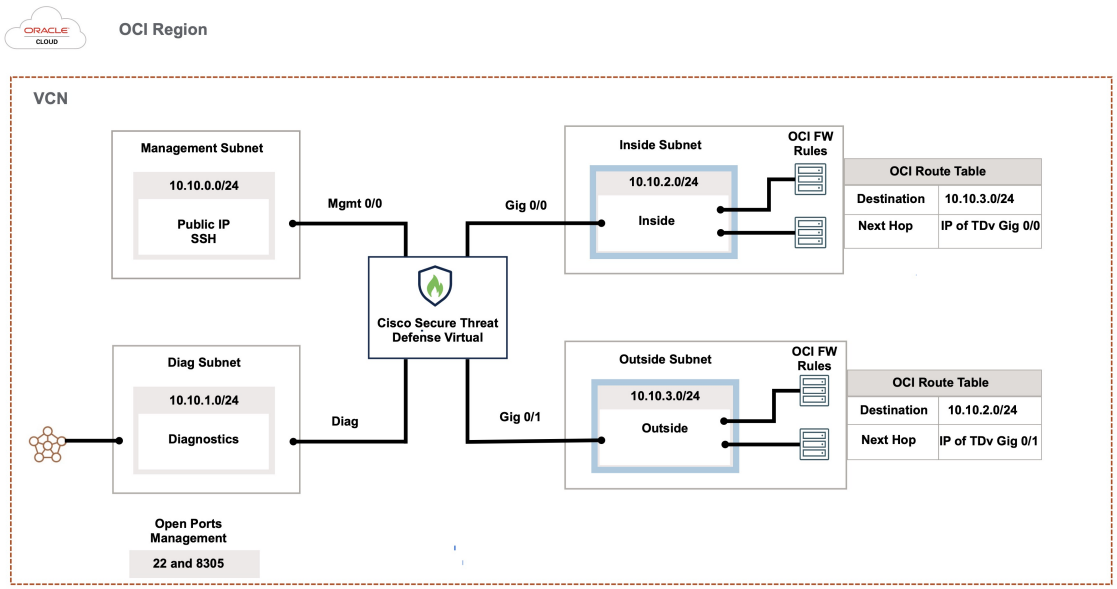
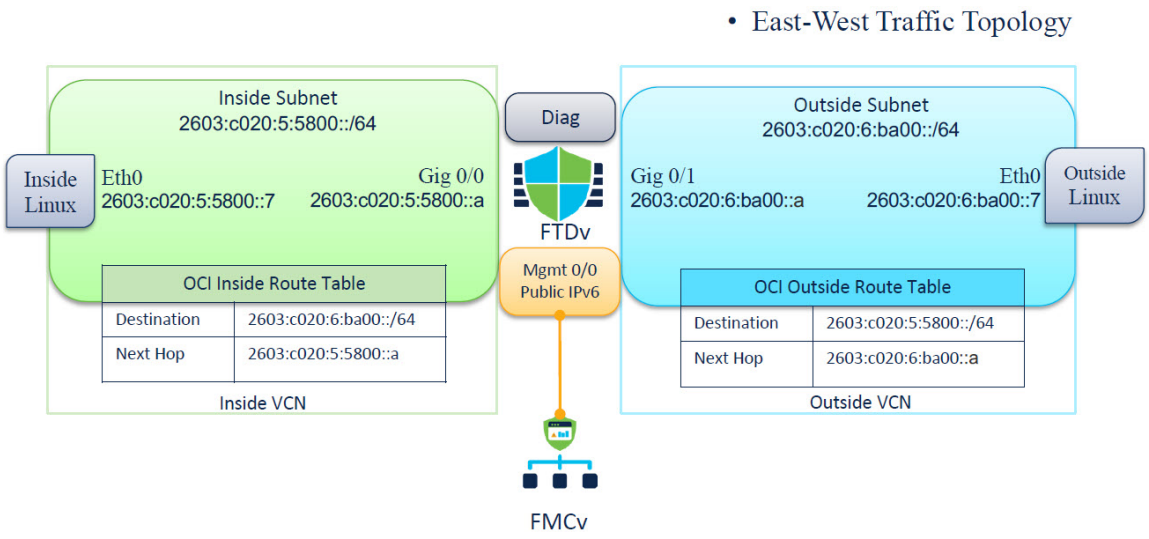


图 *2: VCN* 中具有四个子网的 *OCI* 部署示例 *Threat Defense Virtual*



注释 在单个 VCN 中使用四个子网时，必须将特定于子网的路由添加到与该子网关联的路由表中。

Threat Defense Virtual IPv6 部署拓扑



如何管理 Cisco Secure Firewall Threat Defense Virtual 设备

您有两个选择来管理您的 Cisco Secure Firewall Threat Defense Virtual。

Cisco Secure Firewall Management Center

如果要管理大量设备或要使用 威胁防御 支持的更复杂的功能和配置，请使用 管理中心（而不是集成的 设备管理器）来配置您的设备。

重要事项 您不能同时使用 设备管理器 和 管理中心 来管理 威胁防御 设备。在启用 设备管理器 集成管理功能后，将无法使用 管理中心 来管理 威胁防御 设备，除非您禁用本地管理功能并重新配置管理功能以使用 管理中心。另一方面，当您向 威胁防御 注册 管理中心 设备时，设备管理器 载入管理服务会被禁用。

注意 目前，思科不提供将 设备管理器 配置迁移到 管理中心 的选项，反之亦然。选择为 威胁防御 设备配置的管理类型时，请考虑这一点。

Cisco Secure Firewall 设备管理器

设备管理器 板载集成的管理器。

设备管理器 是基于 Web 的配置界面，包含在某些 威胁防御 设备上。设备管理器可以配置小型网络最常用软件的基本功能。此产品专为包括一台或几台设备的网络而设计，在这种网络中，无需使用高功率多设备管理器来控制包含许多 威胁防御 设备的大型网络。

注释 有关支持 设备管理器 的 威胁防御 设备的列表，请参阅《Cisco Secure Firewall 设备管理器配置指南》。

配置 OCI 环境

您可以为 Threat Defense Virtual 部署配置虚拟云网络 (VCN)，具体如下：

- **多个 VCN (Multiple VCNs)** - 至少需要四个 VCN，每个 threat defense virtual 接口各一个。这允许在不同网络之间进行隔离的流量检测。
- **带子网的单个 VCN (Single VCN with Subnets)** - 或者，您可以配置带四个子网的单个 VCN，每个 Threat Defense Virtual 接口各一个。在此配置中，防火墙可以使用关联的路由表检查和控制同一 VCN 中子网之间的流量。这使您可以在使用单个 VCN 时有效地管理子网间流量。

您可以继续执行以下程序来完成管理 VCN。然后返回到**网络 (Networking)**，为诊断接口、内部接口和外部接口创建 VCN。

过程

步骤 1 登录 OCI 并选择您的区域。

OCI 划分为彼此隔离的多个区域。区域显示在屏幕的右上角。一个区域中的资源不会出现在另一个区域中。请定期检查以确保您在预期的区域内。

步骤 2 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)**，然后点击**创建 VCN (Create VCN)**。

步骤 3 输入 VCN 的描述性**名称**，例如 *FTDv-Management*。

步骤 4 输入 VCN 的 **CIDR 块**。

a) IP 地址的 IPv4 CIDR 块。CIDR（无类别域间路由）是 IP 地址及其关联路由前缀的紧凑表示。例如，10.0.0.0/24。

注释
在此 VCN 中使用 DNS 主机名。

b) IP 地址的 IPv6 CIDR 块。CIDR（无类别域间路由）是 IP 地址及其关联路由前缀的紧凑表示。例如，[::/0]。

c) 选择 IPv6 CIDR 块作为 Oracle 为虚拟云网络分配的 IPv6/56 前缀。

步骤 5 点击**添加 IPv6 CIDR 块 (Add IPv6 CIDR Block)** 以添加新的 IPv6 块。

步骤 6 添加 VCN 的 IPv6 前缀，例如 */54*。

步骤 7 点击**创建 VCN (Create VCN)**。

下一步做什么

继续执行以下程序以完成管理 VCN。完成管理 VCN 后，您将为诊断接口、内部接口和外部接口创建 VCN。

注释 从导航菜单中选择服务后，左侧的菜单包括隔间列表。隔间可帮助您组织资源，以便更轻松地控制对资源的访问。您的根隔间由Oracle在调配租用时为您创建。管理员可以在根隔间中创建更多隔间，然后添加访问规则以控制哪些用户可以在其中查看和执行操作。有关详细信息，请参阅 Oracle 文档管理隔间。

创建网络安全组

网络安全组由一组 vNIC 和一组应用于这些 vNIC 的安全规则组成。

过程

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **网络安全组 (Network Security Groups)**，然后点击**创建网络安全组 (Create Network Security Group)**。

步骤 2 输入网络安全组的描述性**名称**，例如 *FTDv-Mgmt-Allow-22-8305*。

步骤 3 点击**下一步 (Next)**。

步骤 4 添加安全规则：

a) 添加规则以允许 TCP 端口 22 用于 SSH 访问。

b) 添加规则以允许 TCP 端口 8305 用于 HTTPS 访问。

可以通过 管理中心 管理 threat defense virtual，这需要为 HTTPS 连接打开端口 8305。

注释
您可以将这些安全规则应用于管理接口/VCN。

步骤 5 点击**创建 (Create)**。

创建互联网网关

要使管理子网可公开访问，则需要互联网网关。

过程

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **互联网网关 (Internet Gateways)**，然后点击**创建互联网网关 (Create Internet Gateway)**。

步骤 2 输入您的互联网网关的描述性**名称**，例如 *FTDv-IG*。

步骤 3 点击**创建互联网网关 (Create Internet Gateway)**。

步骤 4 将路由添加至互联网网关：

a) 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **路由表 (Route Tables)**。

b) 点击默认路由表的链接以添加路由规则。

c) 点击**添加路由规则 (Add Route Rules)**。

d) 从**目标类型 (Target Type)** 下拉列表中，选择**互联网网关 (Internet Gateway)**。

e) 输入目标 IPv4 CIDR 块，例如 0.0.0.0/0。

f) 输入目标 IPv6 CIDR 块，例如 [::/0]。

g) 从**目标互联网网关 (Target Internet Gateway)** 下拉列表中选择您创建的网关。

h) 点击**添加路由规则 (Add Route Rules)**。

创建子网

每个 VCN 至少有一个子网。您将为管理 VCN 创建一个管理子网。诊断 VCN 还需要一个诊断子网，内部 VCN 需要一个内部子网，外部 VCN 需要一个外部子网。

如果使用一个 VCN，则要在 VCN 内创建管理子网、诊断子网、内部子网和外部子网。

过程

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **子网 (Subnets)**，然后点击**创建子网 (Create Subnet)**。

步骤 2 输入子网的描述性**名称 (Name)**，例如管理 *(Management)*。

步骤 3 选择**子网类型 (Subnet Type)**（保留建议的默认值**区域 (Regional)**）。

步骤 4 输入 **CIDR 块 (CIDR Block)**，例如 10.10.0.0/24。子网的内部（非公共）IP 地址可从此 CIDR 块获取。

a) 如果要启用 IPv6，则选中**启用 IPv6 CIDR 块 (ENABLE IPv6 CIDR BLOCK)** 复选框。

b) 在 **IPv6 CIDR 块 (IPv6 CIDR Block)** 中，输入 IPv6 前缀范围。

步骤 5 从**路由表 (Route Table)** 下拉列表中选择您之前创建的路由表之一。

步骤 6 为您的子网选择**子网访问 (Subnet Access)**。

对于“管理”(Management) 子网，这必须是**公共子网 (Public Subnet)**。

步骤 7 选择 **DHCP 选项 (DHCP Option)**。

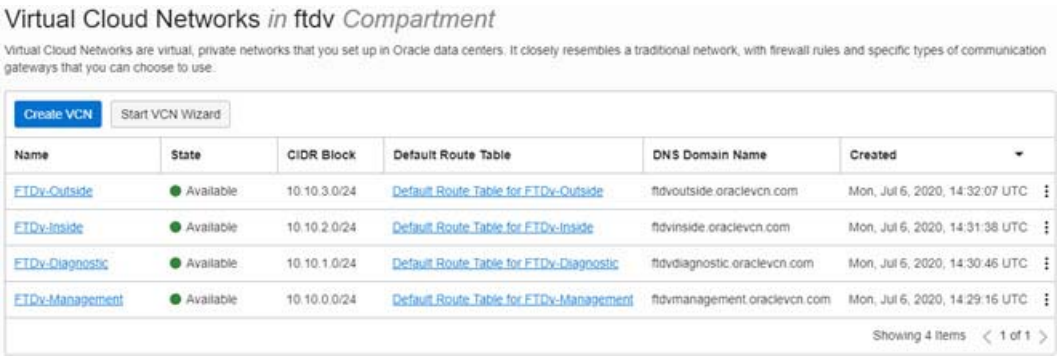
步骤 8 选择您之前创建的**安全列表**。

步骤 9 点击**创建子网 (Create Subnet)**。

下一步做什么

配置管理 VCN（管理、诊断、内部、外部）后，您便可以启动 threat defense virtual。有关 threat defense virtual VCN 配置的示例，请参见下图。

图 *3: threat defense virtual* 虚拟云网络



使用 Cloud Shell 配置 IPv6 网关地址

在 OCI 中，每个子网都有一个唯一的 IPv6 网关地址，您必须在 threat defense virtual 中配置该地址，IPv6 流量才会正常工作。此网关地址可从在云外壳中运行 OCI 命令的子网详细信息进行检索。

在 OCI 上部署 Threat Defense Virtual

过程

步骤 1 转至 **OCI** > **打开 CloudShell（OCI 云终端）(Open CloudShell [OCI Cloud Terminal])** 。

步骤 2 执行以下命令以便从子网获取 IPv6 详细信息：

```
oci network subnet get  -subnet_id <subnet_OCID>
```

步骤 3 从命令结果中查找 `ipv6-virtual-router-ip` 键。

步骤 4 复制该键的值并根据需要使用它。

在 OCI 上部署 Threat Defense Virtual

使用 Oracle Cloud 市场中的 Cisco Firepower NGFW 虚拟防火墙 (NGFWv) 产品通过计算实例在 OCI 上部署 threat defense virtual。根据 CPU 数量、内存量和网络资源等特征来选择最合适的计算机形状。

过程

步骤 1 登录 OCI 门户。

区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**市场 (Marketplace)** > **应用程序 (Applications)**。

步骤 3 在市场中搜索“Cisco Firepower NGFW virtual firewall (NGFWv)”，然后选择产品。

步骤 4 查看条款和条件，然后选中**我已阅读并接受的Oracle使用条款和合作伙伴条款和条件 (I have reviewed and accept the Oracle Terms of Use and the Partner terms and conditions)** 复选框。

步骤 5 点击**启动实例 (Launch Instance)**。

步骤 6 输入您的实例的描述性**名称**，例如 *FTDv-6-7*。

步骤 7 点击**更改形状 (Change Shape)**，然后选择包含 threat defense virtual 所需 CPU 数量、RAM 量和所需接口数量的形状，例如 VM.Standard2.4（请参阅概述，第 2 页）。

步骤 8 从**虚拟云网络 (Virtual Cloud Network)** 下拉列表中选择管理 VCN。

步骤 9 从**子网 (Subnet)** 下拉列表中选择管理子网（如果未自动填充）。

步骤 10 选中**使用网络安全组控制流量 (Use Network Security Groups to Control Traffic)**，然后选择为管理 VCN 配置的安全组。

步骤 11 点击**分配公共 IP 地址 (Assign a Public Ip Address)** 单选按钮。

步骤 12 在**添加 SSH 密钥 (Add SSH keys)** 下，点击**粘贴公共密钥 (Paste Public Keys)** 单选按钮并粘贴 SSH 密钥。

基于 Linux 的实例使用 SSH 密钥对而不是密码来对远程用户进行身份验证。密钥对包括私钥和公共密钥。您可以在创建实例时将私钥保留在计算机上并提供公共密钥。有关准则，请参阅管理 Linux 实例上的密钥对。

步骤 13 点击**显示高级选项 (Show Advanced Options)** 链接以展开选项。

步骤 14 在**初始化脚本 (Initialization Script)** 下，点击**粘贴云初始化脚本 (Paste Cloud-Init Script)** 单选按钮来为 threat defense virtual 提供 day0 配置。day0 配置会在首次引导 threat defense virtual 期间应用。

以下示例显示您可以在**云初始化脚本 (Cloud-Init Script)** 字段中复制和粘贴的示例 day0 配置：

```
{
"Hostname": "ftdv-oci",
"AdminPassword": "myPassword@123456",
"FirewallMode": "routed",
"IPv4Mode": "dhcp",
"IPv6Mode": "dhcp",
"ManageLocally":"No",
"FmcIp": "1.2.3.4",
"FmcRegKey": "cisco123reg",
"FmcNatId": "cisco123nat"
}
```

- **FmcRegKey** - 这是一次性使用的注册密钥，用于将设备注册到 管理中心。该注册密钥是任何用户定义的字母数字值，最长 37 个字符。
- **FmcNatId** - 这是一个唯一的一次性字符串（用户定义）。如果设备和 管理中心 之间被 NAT 设备分开，则必须输入唯一的 NAT ID 和唯一的注册密钥。

步骤 15 点击**创建 (Create)**。

下一步做什么

监控 threat defense virtual 实例，点击**创建 (Create)** 按钮后，状态会显示为“正在调配”(Provisioning)。

重要事项 监控状态非常重要。一旦 threat defense virtual实例从调配变为运行状态，您需要在 threat defense virtual 启动完成之前根据需要连接 VNIC。

连接接口

threat defense virtual会进入运行状态并连接一个 VNIC（请参阅**计算 (Compute)** > **实例 (Instances)** > **实例详细信息 (Instance Details)** > **连接的 VNIC (Attached VNICs)**）。这称为主 VNIC，并会映射到管理 VCN。在 threat defense virtual 完成首次启动之前，您需要为之前创建的其他 VCN 子网（诊断、内部、外部）连接 VNIC，以便在 threat defense virtual 上正确检测 VNIC。

过程

步骤 1 选择新启动的 threat defense virtual实例。

步骤 2 依次选择**连接的 VNIC (Attached VNICs)** > **创建 VNIC (Create VNIC)**。

步骤 3 输入 VNIC 的描述性**名称 (Name)**，例如 *Inside*。

步骤 4 从**虚拟云网络 (Virtual Cloud Network)** 下拉列表中选择 VCN。

步骤 5 从**子网 (Subnet)** 下拉列表选择您的子网。

步骤 6 选中**使用网络安全组控制流量 (Use Network Security Groups to Control Traffic)**，然后选择为所选 VCN 配置的安全组。

步骤 7 选中**跳过源目标 选中**使用网络安全组控制流量 (Use Network Security Groups to Control Traffic)。

步骤 8 （可选）指定**专用 IP 地址**。仅当您要为 VNIC 选择特定 IP 时，才需要执行此操作。

如果未指定 IP，OCI 将从您分配给子网的 CIDR 块分配 IP 地址。

步骤 9 点击**保存更改 (Save Changes)** 以创建 VNIC。

步骤 10 对部署所需的每个 VNIC 重复此程序。

为连接的 VNIC 添加路由规则

将路由表规则添加到诊断、内部和外部路由表。

过程

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)**，然后点击与 VCN 关联的默认路由表（内部或外部）。

步骤 2 点击**添加路由规则 (Add Route Rules)**。

步骤 3 从**目标类型 (Target Type)** 下拉列表中，选择**专用 IP (Private IP)**。

步骤 4 从**目的类型 (Destination Type)** 下拉列表中选择**CIDR 块 (CIDR Block)**。

步骤 5 输入**目标 CIDR 块**，例如 0.0.0.0/0。

步骤 6 在**目标选择 (Target Selection)** 字段中输入 VNIC 的私有 IP 地址。

如果未向 VNIC 明确分配 IP 地址，则可以从 VNIC 详细信息（**计算 (Compute)** > **实例 (Instances)** > **实例详细信息 (Instance Details)** > **连接的 VNIC (Attached VNICs)**）中查找自动分配的 IP 地址。

步骤 7 点击**添加路由规则 (Add Route Rules)**。

如果要通过互联网网关配置 IPv6 互联网访问，请执行以下操作：

a) 从**目标类型 (Target Type)** 下拉列表中，选择**互联网网关 (Internet Gateway)**。
b) 在**目标 CIDR 块**中，指定 IP 地址
c) 从**目标互联网网关 (Target Internet Gateway)** 下拉列表中，选择现有互联网网关隔间或创建新的互联网网关隔间。

步骤 8 对部署所需的每个 VNIC 重复此程序。

注释
如果使用通过 DHCP 的路由规则或 IPv6 地址前缀配置的 IPv6 地址为 /128，则必须在 threat defense virtual 路由表中添加以下路由。

ipv6 route <interface_name> <interface_subnet_CIDR> <ipv6_virtual_router_ip>

示例：

- `ipv6 route inside 2603:c020:5:5800::/64 fe80::200:17ff:fe96:921b`
- `ipv6 route outside 2603:c020:6:ba00::/64 fe80::200:17ff:fe21:748c`

部署 Auto Scale 解决方案

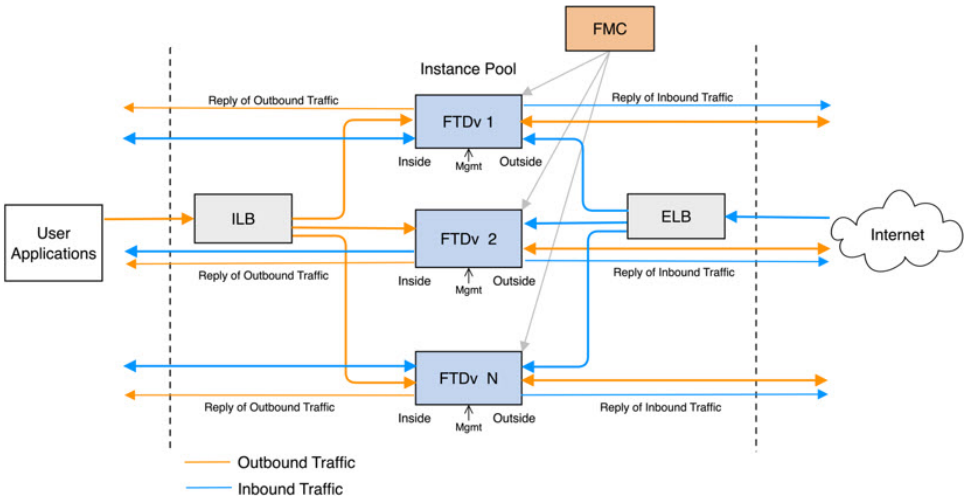
以下各节介绍 Auto Scale 解决方案的组件如何对 OCI 上的 threat defense virtual 发挥作用。

Auto Scale 使用案例

OCI 上 threat defense virtual 自动扩展解决方案的使用案例如下图所示。面向互联网的负载均衡器将有一个使用侦听程序和目标组的组合启用的端口的公共 IP 地址。

可以通过 NAT 规则对流量进行基于端口的分叉。下文将对此进行解释。

图 *4: Cisco Secure Firewall Threat Defense Virtual Auto Scale* 使用案例图



适用范围

本文档介绍了部署适用于 OCI 的 threat defense virtual Auto Scale 解决方案的详细步骤。

重要事项

- 请先阅读整个文档，然后再开始部署。
- 在开始部署之前，请确保满足前提条件。
- 请确保遵守此处所述的步骤和执行顺序。

前提条件

权限和策略

以下是实施解决方案所需的 OCI 权限和策略：

1. **用户和组**

注释 您必须是 OCI 用户或租户管理员才能创建用户和组。

创建 Oracle 云基础设施用户账户和用户账户所属的组。如果存在具有用户账户的相关组，则无需再进行创建。有关创建用户和组的说明，请参阅创建组和用户。

2. **组策略**

您需要创建策略，然后将其映射到组。要创建策略，请转至 **OCI** > **身份和安全 (Identity & Security)** > **策略 (Policies)** > **创建策略 (Create Policy)**。创建以下策略并将其添加到所需的组中：

- 允许组 <*Group_Name*> 使用隔离专区 <*Compartment_Name*> 中的指标
- 允许组 <*Group_Name*> 管理隔离专区 <*Compartment_Name*> 中的警报
- 允许组 <*Group_Name*> 管理隔离专区 <*Compartment_Name*> 中的主题
- 允许组 <*Group_Name*> 检查隔离专区 <*Compartment_Name*> 中的指标
- 允许组 <*Group_Name*> 读取隔离专区 <*Compartment_Name*> 中的指标
- 允许组 <*Group_Name*> 使用隔离专区 <*Compartment_Name*> 中的标记命名空间
- 允许组 <*Group_Name*> 读取隔离专区 <*Compartment_Name*> 中的日志组
- 允许组 <*Group_Name*> 使用隔离专区 <*Compartment_Name*> 中的实例池
- 允许组 <*Group_Name*> 使用租户中的 Cloud Shell
- 允许组 <*Group_Name*> 读取租户中的对象存储命名空间
- 允许组 <*Group_Name*> 管理租户中的存储库

注释 您也可以在租户级别创建策略。您可以自行决定如何提供所有的权限。

3. **Oracle 功能的权限**

   要让 Oracle 功能能够访问另一个 Oracle 云基础设施资源，请将该功能包含在动态组中，然后创建一个策略以授予该动态组对该资源的访问权限。

4. **创建动态组**

   要创建动态组，请转至 **OCI** > **身份和安全 (Identity & Security)** > **动态组 (Dynamic Group)** > **创建动态组 (Create Dynamic Group)**

   在创建动态组时指定以下规则：

   ```
   ALL {resource.type = 'fnfunc', resource.compartment.id = '<Your_Compartment_OCID>'}
   ```

   有关动态组的更多详细信息，请参阅：

   - https://docs.oracle.com/en-us/iaas/Content/Functions/Tasks/functionsaccessingociresources.htm
   - https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingdynamicgroups.htm

5. **为动态组创建策略**

   要添加策略，请转至 **OCI** > **身份和安全 (Identity & Security)** > **策略 (Policies)** > **创建策略 (Create Policy)**。将以下策略添加到组：

   ```
   允许动态组 <Dynamic_Group_Name> 管理隔离专区 <Compartment_OCID> 中的所有资源
   ```

从 GitHub 下载文件

FTDv – OCI Autoscale 解决方案已作为 GitHub 存储库提供。您可以从存储库中提取或下载文件。

Python3 环境

可以在克隆存储库中找到 *make.py* 文件。此程序会将 Oracle 功能和模板文件压缩为 Zip 文件；将它们复制到目标文件夹。为了执行这些任务，应配置 Python 3 环境。

注释 此 Python 脚本只能用于 Linux 环境中。

基础设施配置

必须配置以下选项：

1. **VCN**

   根据 FTDv 应用的需要创建 VCN。创建具有互联网网关的 VCN，该网关至少有一个通过到互联网的路由连接的子网。

有关创建 VCN 的信息，请参阅https://docs.oracle.com/en-us/iaas/Content/GSG/Tasks/creatingnetwork.htm。

2. **应用程序子网**

   根据需要为 FTDv 应用创建子网。要根据此使用案例实施解决方案，FTDv 实例需要 4 个子网才能运行。

   有关创建子网的信息，请参阅 https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingVCNs_topic-Overview_of_VCNs_and_Subnets.htm#。

3. **外部子网**

   子网应该具有能够通过“0.0.0.0/0”连接互联网网关的路由。此子网包含思科 FTDv 的外部接口和面向互联网的负载均衡器。确保为出站流量添加 NAT 网关。

   有关详情，请参阅以下文档：

   - https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingIGs.htm
   - https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/NATgateway.htm#To_create_a_NAT_gateway

4. **内部子网**

   这与具有或没有 NAT/互联网网关的应用程序子网类似。

注释 对于 FTDv 运行状况探测，您可以通过端口 80 来访问元数据服务器 (169.254.169.254)。

5. **管理子网**

   管理子网应是公共子网，这样它才能支持对 FTDv 的 SSH 可访问性。

6. **Function 子网**

   此子网用于 Oracle Functions 部署。

注释 此子网必须具有到 NAT GW（而不是互联网 GW）的 `0.0.0.0/0` 路由。

必须在 Management Center Virtual 和 Threat Defense Virtual的 NSG（网络安全组）中允许此子网的 NAT GW 的公共 IP。

7. **安全组 - FTDv 实例的网络安全组**

   为 FTDv 实例配置安全组，以允许 Oracle 功能（在同一 VCN 中）执行到 FTDv 的管理地址的 SSH 连接。

8. **对象存储命名空间**

此对象存储命名空间用于托管静态网站，包含 configuration.txt 文件。您必须为 configuration.txt 文件创建预身份验证请求。此预身份验证 URL 可在模板部署期间使用。

注释 确保 FTDv 实例可通过 HTTP URL 访问已上传的以下配置。

当 FTDv 启动时，它会执行以下命令 `$ copy /noconfirm <configuration.txt file's pre-authenticated request URL > disk0:Connfiguration.txt`

此命令支持要使用 configuration.txt 文件配置的 FTDv 启动。

Cisco Secure Firewall Management Center必备条件

您可以使用 Cisco Secure Firewall Management Center 来管理 threat defense virtual，这是一个功能齐全的多设备管理器。threat defense virtual 向您分配给 threat defense virtual 虚拟机的管理接口上的 FMC 注册并与之通信。

创建 threat defense virtual 配置和管理所需的对象，包括在多台设备上部署策略和安装更新的设备组。设备组上应用的所有配置都将被推送到 threat defense virtual 实例。

以下各节简要概述准备 管理中心 的基本步骤。有关程序的完整信息，请参阅《*Cisco Secure Firewall Management Center* 配置指南》。准备 管理中心 时，请确保记录以下信息：

- Cisco Secure Firewall Management Center 公用 IP 地址
- 用户名和密码（如果启用了基于内存的扩展，则必须提供 2 个用户凭证）
- 安全区名称
- Cisco Secure Firewall Management Center 访问策略名称
- Cisco Secure Firewall Management Center NAT 策略名称
- 设备组名称

在 Cisco Secure Firewall Management Center 中创建用户

在 Cisco Secure Firewall Management Center 中创建具有 Admin 权限的新用户，以便仅供 Autoscale Manager 使用。

注释 您必须有一个专用于 threat defense virtual Autoscale 解决方案的 Cisco Secure Firewall Management Center 用户账户，以防止与其他 FMC 会话发生冲突。

过程

在 Cisco Secure Firewall Management Center 中创建具有 Admin 权限的新用户。选择**系统 (System)** > **用户 (Users)**，然后点击**创建用户 (Create User)**。用户名必须对 Linux 有效：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不应以连字符 (-) 开头；必须包含字母；不应包含句点 (.)、符号 (@) 或斜线 (/)

根据环境需要完成用户选项。有关完整信息，请参阅 《*Cisco Secure Firewall Management Center* 配置指南》。

创建设备组

可以使用设备组轻松分配策略，并在多台设备上安装更新。应创建一个设备组，然后应对其应用规则。设备组上应用的所有配置都将被推送到 threat defense virtual 实例。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 从**添加 (Add)** 下拉菜单中选择**添加组 (Add Group)**。

步骤 3 输入设备组名称。

步骤 4 点击**确定 (Ok)** 以创建设备组。

创建网络和主机对象

创建以下要用于 threat defense virtual 配置的对象。

过程

步骤 1 创建名为 *oci-metadata-server* 且 IP 为 *169.254.169.254* 的主机。

步骤 2 创建名为 health-check-port 且值为 8080 的端口，或根据需要创建任何其他端口。

步骤 3 创建内部接口，依次选择**接口 (Interface)** > **安全区域 (Security Zone)**。选择**已路由 (Routed)** 作为类型。为接口提供名称，例如 *inside-sz*。

步骤 4 创建外部接口，依次选择**接口 (Interface)** > **安全区域 (Security Zone)**。选择**已路由 (Routed)** 作为类型。为接口提供名称，例如 *outside-sz*。

创建 NAT 策略

创建 NAT 策略并创建必要的 NAT 规则，以便将流量从外部接口转发到应用程序，然后将此策略连接到您为 Auto Scale 创建的设备组。

过程

步骤 1 选择**设备 (Devices)** > **NAT**

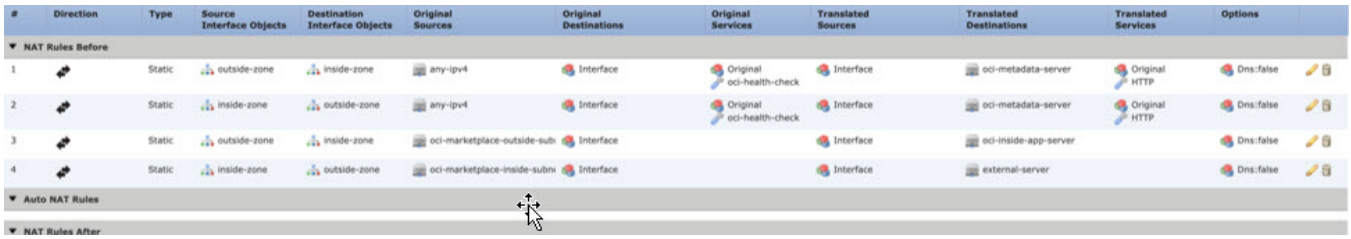
步骤 2 从**新策略**下拉列表中，选择**威胁防御 NAT**。

步骤 3 在**名称 (Name)** 中输入唯一的名称。

步骤 4 输入**说明 (Description)**（可选）。

步骤 5 配置 NAT 规则。有关如何创建 NAT 规则和应用 NAT 策略的指南，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的为威胁防御配置 NAT。下图显示了设置规则的基本方法。

图 *5: NAT* 规则



步骤 6 点击**保存 (Save)**。

创建 NAT 规则

典型的 NAT 规则会将内部地址转换为外部接口 IP 地址上的端口。这类 NAT 规则称为接口端口地址转换 (PAT)。有关详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的为威胁防御配置 NAT。

配置 NAT 策略中所需的以下 2 条强制性规则：

过程

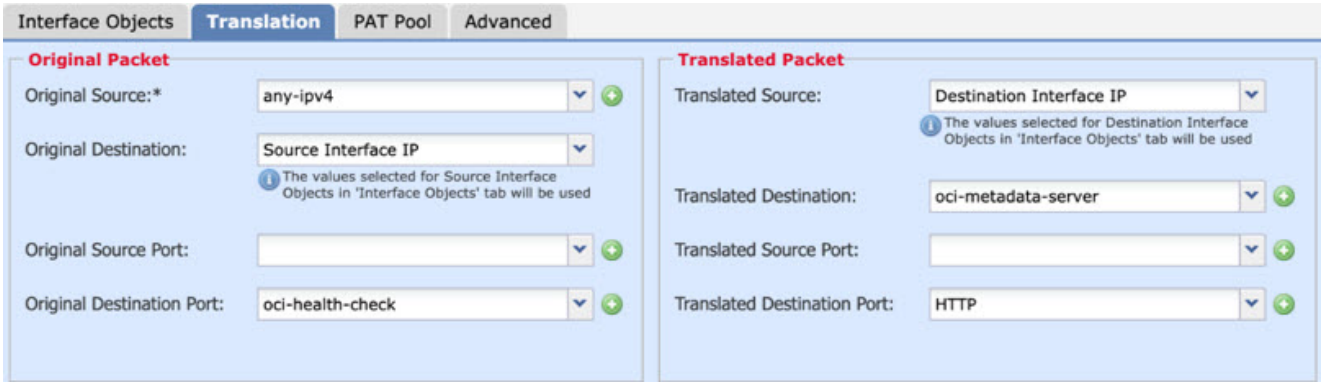
步骤 1 为入站运行状况检查配置以下 NAT 规则：

- 源区域：外部区域
- 目标区域：内部区域
- 原始源：any-ipv4
- 原始目标：源接口 IP

- 原始源端口：默认
- 原始目标端口：health-check-port
- 已转换的源：目标接口 IP
- 已转换的目标：oci-metadata-server
- 已转换的源端口：默认
- 已转换的目标端口：HTTP

下图显示了用于入站运行状况检查的 NAT 规则。

图 *6:* 入站运行状况 *NAT* 规则

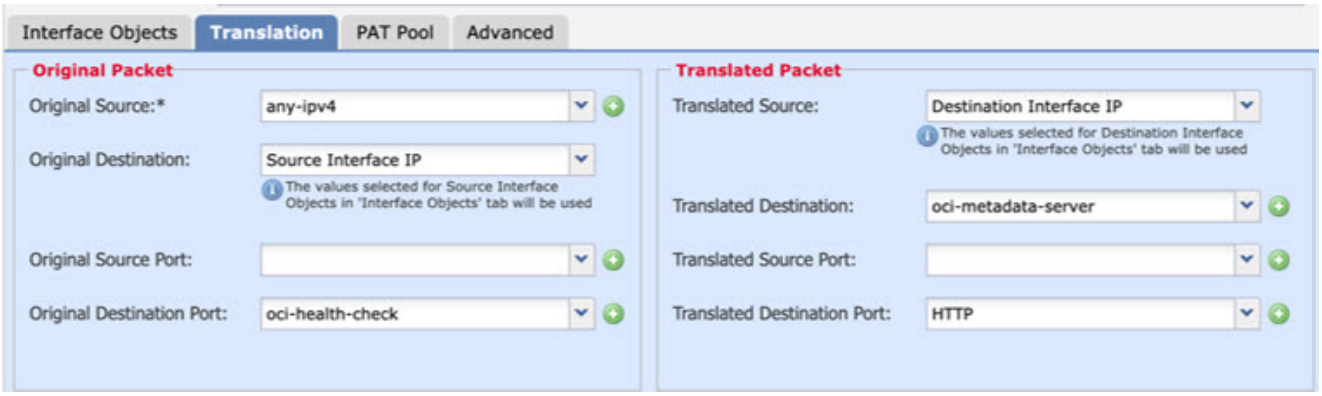


步骤 2 为出站运行状况检查配置以下 NAT 规则。

- 源区域：内部区域
- 目标区域：外部区域
- 原始源：any-ipv4
- 原始目标：源接口 IP
- 原始源端口：默认
- 原始目标端口：health-check-port
- 已转换的源：目标接口 IP
- 已转换的目标：oci-metadata-server
- 已转换的源端口：默认
- 已转换的目标端口：HTTP

下图显示了用于出站运行状况检查的 NAT 规则。

图 7: 出站运行状况检查 *NAT* 规则



同样，也可以为数据流量添加任何 NAT 规则，并将其推送到 threat defense virtual 设备上。

创建访问策略

配置访问控制以允许从内部到外部的流量。可以创建具有所有必需策略的访问策略，应允许运行状况端口对象，以便允许此端口上的流量到达设备。在访问控制策略中，访问控制规则提供在多台受管设备之间处理网络流量的精细方法。规则的正确配置和排序对构建有效的部署至关重要。请参阅《Cisco Secure Firewall Management Center 设备配置指南》 的访问控制规则最佳实践。

使用**策略分配**将设备组（作为前提条件创建）分配给访问策略。

过程

步骤 1 依次选择**策略** > **访问控制**。

步骤 2 点击**新建策略**。

步骤 3 在名称 (Name) 和说明 (Description)（可选）中输入唯一名称和说明。

步骤 4 为部署配置安全设置和规则。有关详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的访问控制。

加密密码

注释 有关此程序的详细信息，请参阅创建保管库和密钥。

FTDv 的密码用于配置自动扩展时使用的所有 FTDv 实例，并且它还用于为多个配置目的创建 Rest API 调用连接。

因此，您需要不时地保存和处理密码。由于密码更改频繁且存在漏洞，因此不允许以纯文本格式编辑或保存密码。密码只能采用加密格式。

要以加密形式获取密码，请执行以下操作：

过程

步骤 1 创建保险库。

OCI 保险库提供安全创建和保存主加密密钥的服务，以及使用它们进行加密和解密的方法。因此，应在与 Autoscale 解决方案的其余部分相同的隔离专区中创建保险柜（如果尚未创建）。

转至 **OCI > 身份和安全 (Identity & Security) > 保管库 (Vault) > 选择或创建新保管库 (Choose or Create New Vault)**

。

步骤 2 创建主加密密钥。

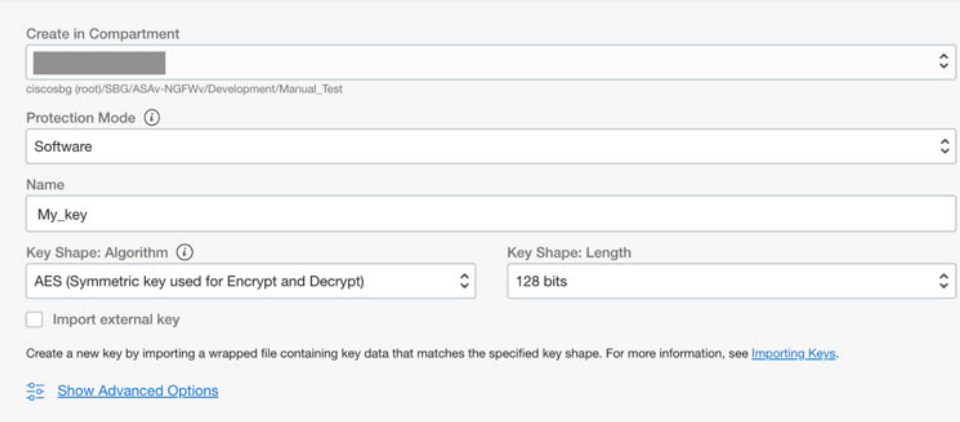
需要使用主加密密钥才能加密纯文本密码。

转至 **OCI > 身份和安全 (Identity & Security) > 保管库 (Vault) > 选择或创建密钥 (Choose or Create Key)**

从任意给定算法中选择任意长度的密钥。

1. AES - 128、192、256
2. RSA - 2048、3072、4096
3. ECDSA - 256、384、521

图 *8:* 创建密钥



步骤 3 创建加密密码。。

1. 转至 **OCI > 打开 CloudShell（OCI 云终端）(Open CloudShell [OCI Cloud Terminal])**
2. 通过替换 <*Password*> 作为密码来执行以下命令。

```
echo -n '<Password>' | base64
```

3. 从选定的保险库中，复制加密终端和主加密密钥 OCID。替换以下值，然后执行 encrypt 命令：
   - 将 KEY_OCID 替换为您的密钥的 OCID
   - 将 Cryptographic_Endpoint_URL 替换为您的保险库的加密终端 URL
   - 将密码替换为您的密码

   加密命令

   ```
   oci kms crypto encrypt --key-id Key_OCID --endpoint
   Cryptographic_Endpoint_URL --plaintext <base64-value-of-password>
   ```

4. 从上述命令的输出中复制密文，然后根据需要使用它们。

准备 threat defense virtual 配置文件

应用程序可能已部署或其部署计划可用。

过程

步骤 1 在部署之前收集以下输入参数：

参数	数据类型	说明
tenancy_ocid	字符串	您的账户所属的租户的 OCID。要了解如何查找租户 OCID，请参阅此处。 租户 OCID 如下所示 - `ocid1.tenancy.oc1..<unique_ID>`
region	字符串	要在其中创建资源的区域的唯一标识符。 示例 - us-phoenix-1、us-ashburn-1
lb_size	字符串	用于确定外部和内部负载均衡器的总预调配带宽（入口加出口）的模板。 支持的值：100Mbps、10Mbps、10Mbps-Micro、400Mbps、8000Mbps 示例：100Mbps
availability_domain	字符串	示例 - Tpeb:PHX-AD-1、Tpeb:PHX-AD-2 **注释** 要获取可用性域名，请参阅此处。

参数	数据类型	说明
min_and_max_instance_count	逗号分隔值	您希望在实例池中保留的最小和最大实例数。 示例：1,5
autoscale_group_prefix	字符串	用于对通过使用模板创建的所有资源命名的前缀。例如，如果资源前缀为“autoscale”，则所有资源均按会如下方式命名 - autoscale_resource1、autoscale_resource2 等。
mgmt_subnet_ocid	字符串	要使用的管理子网的 OCID。
inside_subnet_ocid	字符串	要使用的内部子网的 OCID。
function_subnet_ocid	字符串	要使用的 Function 子网的 OCID。
outside_subnet_ocid	字符串	要使用的外部子网的 OCID。
mgmt_nsg_ocid	字符串	要使用的管理子网网络安全组的 OCID。
inside_nsg_ocid	字符串	要使用的内部子网网络安全组的 OCID。
outside_nsg_ocid	字符串	要使用的外部子网网络安全组的 OCID。
elb_listener_port	逗号分隔值	外部负载均衡器侦听程序的通信端口列表。 示例： 80
ilb_listener_port	逗号分隔值	内部负载均衡器侦听程序的通信端口列表。 示例： 80
health_check_port	字符串	运行运行状况检查的负载均衡器的后端服务器端口。 示例：8080
instance_shape	字符串	要创建的实例的形状。形状可确定分配给实例的CPU数量、内存量和其他资源。 支持的形状：“VM.Standard2.4”和“VM.Standard2.8”
lb_bs_policy	字符串	用于内部和外部负载均衡器后端的负载均衡器策略。要了解有关负载均衡器策略工作原理的更多信息，请参阅此处 支持的值：“ROUND_ROBIN”、“LEAST_CONNECTIONS”、“IP_HASH”

参数	数据类型	说明
image_name	字符串	用于创建实例配置的市场映像的名称。 默认值：“Cisco Firepower NGFW virtual firewall (NGFWv)” 注释 如果用户想要部署自定义映像，则用户必须配置 custom_image_ocid 参数。
scaling_thresholds	逗号分隔值	用于内向扩展和外向扩展的 CPU 使用率阈值。以逗号分隔输入的形式提供内向扩展和外向扩展阈值。 示例：15,50 其中，15 是内向扩展阈值，50 是外向扩展阈值。
compartment_id	字符串	要在其中创建资源的隔离专区的 OCID。 示例：**ocid1.compartment.oc1..<unique_ID>**
compartment_name	字符串	隔离专区的名称
custom_image_ocid	字符串	如果未使用市场映像，用于创建实例配置的自定义映像的 OCID。 注释 *custom_image_ocid* 是可选参数
ftdv_password	字符串	threat defense virtual 采用加密形式的密码，用于通过 SSH 连接到 threat defense virtual 配置。有关如何加密密码的说明，请参阅配置指南，或参阅此处。
ftdv_license_type	字符串	threat defense virtual 许可证的类型，可以是 BYOL 或 PAYG。目前支持 BYOL。
cryptographic_endpoint	字符串	加密终端是用于解密密码的URL。它可以在保险库中找到。
master_encryption_key_id	字符串	用于加密密码的密钥的 OCID。它可以在保险库中找到。 注释 master_encryption_key_id 和 cryptographic_endpoint 必须属于同一保险库。

参数	数据类型	说明
fmc_ip	字符串	Cisco Secure Firewall Management Center 的 IP 地址。客户用来管理 threat defense virtual 实例的 管理中心 IP。 **注释** 只有当与 *threat defense virtual* 位于同一子网时，管理中心 *IP* 才为专用，否则必须将公共 *IP* 用于所有其他情况。
fmc_username	字符串	管理中心 账户的用户名。每次新的 threat defense virtual 实例出现时，此用户名将用于登录 管理中心 进行配置。
fmc_password	字符串	加密形式的 管理中心 密码。有关如何加密密码的程序，请参阅此处。
fmc_device_group_name	字符串	管理中心 中必须有一个设备组，此 Autoscale 解决方案的所有 threat defense virtual 部分都会被添加到该组中，以便可以将相同的策略和配置应用于所有这些设备。
enable_memory_based_scaling	bool	从 Cisco Secure Firewall Management Center Virtual 发布 threat defense virtual 内存使用情况。通过启用此标志，也可以根据内存利用率进行扩展。默认使用 CPU 利用率。
fmc_metrics_username	字符串	如果您通过启用标志 enable_memory_based_scaling 来选择内存利用率，则需要一个额外的 管理中心 用户账户，因为该账户将持续用于从所有正在运行 threat defense virtual 实例提取内存使用情况。
fmc_metrics_password	字符串	加密形式的额外 管理中心 账户的密码。有关如何加密密码的程序，请参阅此处。
配置文件名称 (Profile Name)		它是 OCI 中的用户配置文件名称。它可以在用户的配置文件部分下找到。示例： “oracleidentitycloudservice/<user> @<mail> .com”
对象存储命名空间		它是在创建租户时创建的唯一标识符。转至 **OCI** > **管理 (Administration)** > **租户详细信息 (Tenancy Details)**
授权令牌		这用作 Docker 登录的密码，授权其将 Oracle-Functions 推送到 OCI 容器注册表中。转至 **OCI** > **身份 (Identity)** > **用户 (Users)** > **用户详细信息 (User Details)** > **身份验证令牌 (Auth Tokens)** > **生成令牌 (Generate Token)**。

步骤 2 使用以下内容来创建 *Configuration.json* 文件：

```
{
  "licenseCaps": ["BASE", "MALWARE", "THREAT"],
  "performanceTier": "FTDv30",
  "fmcIpforDeviceReg": "DONTRESOLVE",
  "RegistrationId": "cisco",
  "NatId": "cisco",
  "fmcAccessPolicyName": "<autoscale-access-policy-name>",
  "fmcNatPolicyName": "<autoscale-nat-policy-name>",
  "fmcInsideNicName": "inside",
  "fmcOutsideNicName": "outside",
  "fmcInsideNic": "GigabitEthernet0/0",
  "fmcOutsideNic": "GigabitEthernet0/1",
  "fmcOutsideZone": "<outside-zone-name>",
  "fmcInsideZone": "<inside-zone-name>",
  "MetadataServerObjectName": "oci-metadata-server",
  "interfaceConfig": [
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
        "name": "inside-zone"
      },
      "mode": "NONE",
      "ifname": "inside",
      "name": "GigabitEthernet0/0"
    },
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
        "name": "outside-zone"
      },
      "mode": "NONE",
      "ifname": "outside",
      "name": "GigabitEthernet0/1"
    }
  ],
  "trafficRoutes": [
    {
      "interface": "outside",
      "network": "any-ipv4",
      "gateway": "",
      "metric": "2"
    },
    {
      "interface": "inside",
      "network": "oci-metadata-server",
      "gateway": "",
      "metric": "1"
    }
  ]
}
```

步骤 3 使用配置设置来更新 *Configuration.json*。

步骤 4 将配置文件上传到对象存储空间。

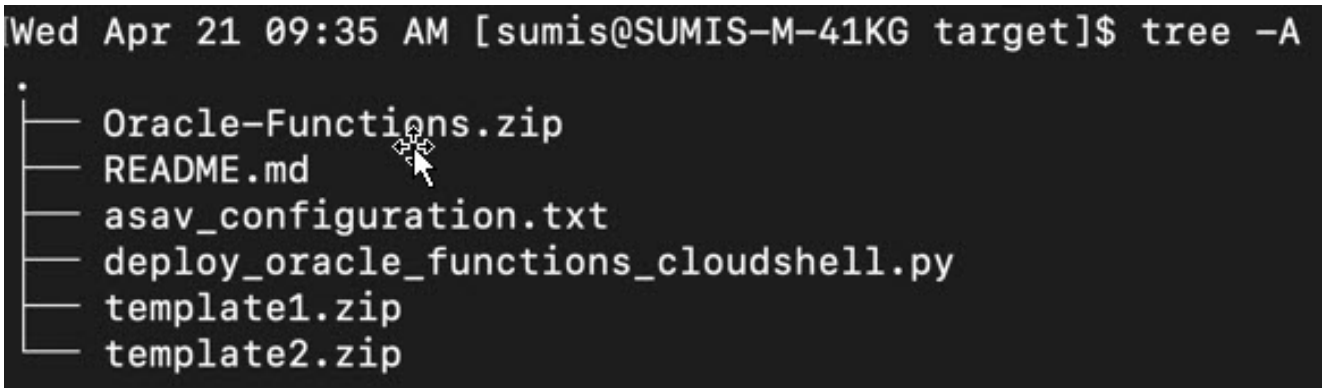
必须将 *configuration.txt* 文件上传到用户创建的对象存储空间，并为上传的文件创建预身份验证请求。

注释
确保在堆栈部署中使用 configuration.txt 的预身份验证请求 URL。

注释
在 OCI 中创建预身份验证 URL 时需要定义到期时间，请确保该时间段足够长，不会在解决方案执行期间到期。

步骤 5 创建 Zip 文件。

可以在克隆存储库中找到 *make.py* 文件。执行 `python3 make.py build` 命令以创建 zip 文件。目标文件夹包含以下文件。



部署 Auto Scale 解决方案

在完成部署的必备步骤后，开始创建 OCI 堆栈。您可以使用 Cloud Shell 执行手动部署或使用 Cloud Shell 部署。您的版本的部署脚本和模板可从 GitHub 存储库获取。

手动部署

端到端 Autoscale 解决方案部署包括三个步骤：部署 Terraform Template-1 堆栈 、部署 Oracle 功能，然后部署 Terraform Template-2。

部署 Terraform Template-1 堆栈

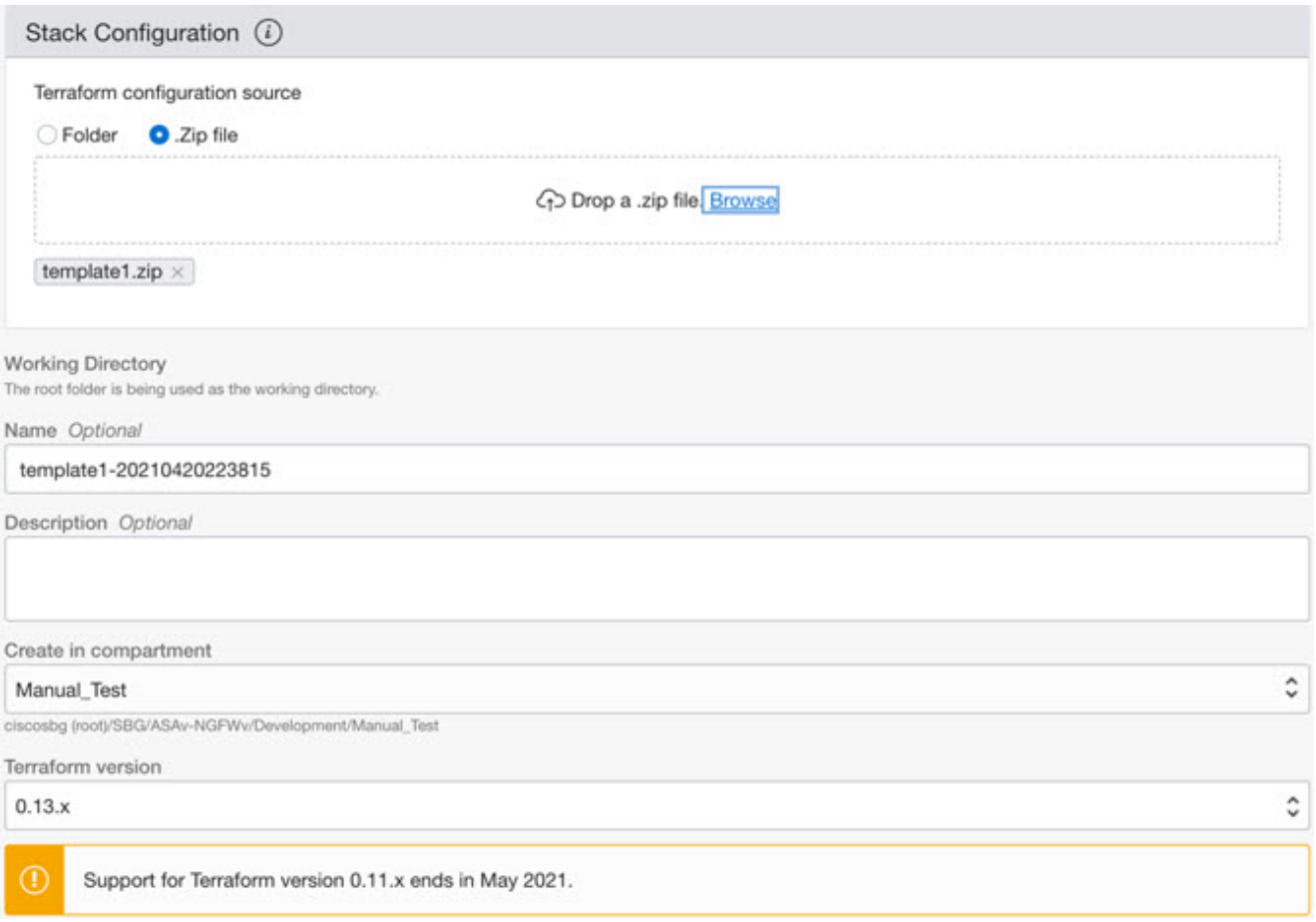
过程

步骤 1 登录 OCI 门户。

区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**开发人员服务 (Developer Service)** > **资源管理器 (Resource Manager)** > **堆栈 (Stack)** > **创建堆栈 (Create Stack)**

选择**我的配置 (My Configuration)**，然后选择目标文件夹中的 *Terraform template1.zip* 文件作为 Terraform 配置源，如下图所示。



步骤 3 在**转换版本 (Transform version)** 下拉列表中，选择 0.13.x 或 0.14.x。

步骤 4 在下一步中，输入步骤 1 中收集的所有详细信息。

注释
输入有效的输入参数，否则堆栈部署可能会在后续步骤中失败。

步骤 5 在下一步中，选择 **Terraform 操作 (Terraform Actions)** > **应用 (Apply)**。

成功部署后，继续部署 Oracle 功能。

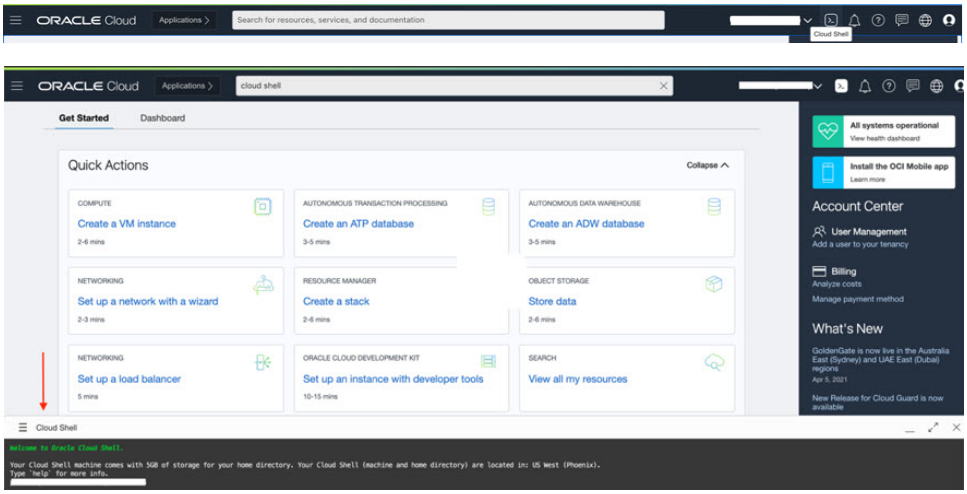
部署 Oracle 功能

注释 只有在 *Terraform Template-1* 部署成功后才能执行此步骤。

在 OCI 中，Oracle 功能会作为 Docker 映像上传，并会保存到 OCI 容器注册表中。在部署时，需要将 Oracle 功能推送到其中一个 OCI 应用（在 Terraform Template-1 中创建）中。

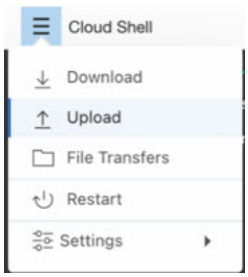
过程

步骤 1 打开 OCI Cloud Shell。



步骤 2 上传 *deploy_oracle_functions_cloudshell.py* 和 *Oracle-Functions.zip*。

从 Cloud Shell 的汉堡菜单中，选择**上传 (Upload)**。



步骤 3 使用 **ls** 命令来验证文件。

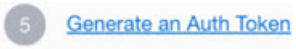
步骤 4 运行 `python3 Deploy_Oracle_Functions.py -h`。`deploy_oracle_functions_cloudshell.py` 脚本需要一些输入参数，可使用 help 参数找到其详细信息，如下图所示。

```
                                $ python3 Deploy_Oracle_Functions.py -h
usage: Deploy_Oracle_Functions.py [-h] -a  -r  -p  -c  -o  -t

*** Script to deploy Oracle Function for OCI ASAv Autoscale Solution ***

Instruction to find values of required arguments:
Application Name: Name of Application created by first Terraform Template
Region Identifier: OCI -> Administration -> Region Management
Profile Name: OCI -> Profile
Compartment OCID: OCI -> Identity -> Compartment -> Compartment Details
Object Storage Namespace: OCI -> Administration -> Tenancy Details
Authorization Token: OCI -> Identity -> Users -> User Details -> Auth Tokens -> Generate Token

optional arguments:
  -h, --help  show this help message and exit
  -a          Name of Application in OCI to which functions will be deployed
  -r          Region Identifier
  -p          Profile Name of User
  -c          Compartment OCID
  -o          Object Storage Namespace
  -t          Authorization Token for Docker Login (*Please Put in Quotes)
```

要运行脚本，请传递以下参数：

表 *3:* 参数和详细信息

参数	详细说明
应用名称	它是 Terraform Template-1 部署创建的 OCI 应用的名称。通过将 Template-1 中给出的“**autoscale_group_prefix**”和后缀“**_application**”组合在一起即可获得其值。
区域标识符	区域标识符是在不同区域的 OCI 中固定的区域代码字。 示例：表示凤凰城的“us-phoenix-1”或表示墨尔本的“ap-melbourne-1”。 要获取所有区域及其区域标识符的列表，请转至 **OCI** > **管理 (Administration)** > **区域管理 (Region Management)**。
配置文件名称	它是 OCI 中的简单用户配置文件名称。 示例：*oracleidentitycloudservice/<user>@<mail>.com* 该名称可以在用户的配置文件部分下找到。
隔离专区 **OCID**	它是隔离专区的 OCID（Oracle 云标识符）。用户拥有 OCI 应用的隔离专区 OCID。 转至 **OCI** > **身份 (Identity)** > **隔离专区 (Compartment)** > **隔离专区详细信息 (Compartment Details)**。
对象存储命名空间	它是在创建租户时创建的唯一标识符。 转至 **OCI** > **管理 (Administration)** > **租户详细信息 (Tenancy Details)**。

参数	详细说明
授权令牌	这用作 Docker 登录的密码，授权其将 Oracle-Functions 推送到 OCI 容器注册表中。在部署脚本中用引号指定令牌。 转至 **OCI** > **身份 (Identity)** > **用户 (Users)** > **用户详细信息 (User Details)** > **身份验证令牌 (Auth Tokens)** > **生成令牌 (Generate Token)**。 出于某种原因，如果您无法查看用户详细信息，请点击**开发人员服务 (Developer services)** > **功能 (Functions)**。转至 Terraform Template-1 创建的应用。点击**开始 (Getting Started)**，然后选择 Cloud Shell 设置，在这些步骤中，您将找到生成身份验证令牌的链接，如下所示。 

步骤 5 通过传递有效的输入参数运行 `python3 Deploy_Oracle_Functions.py` 命令。部署所有的功能需要一些时间。然后，您可以删除该文件并关闭 Cloud Shell。

部署 Terraform Template-2

模板 2 部署与警报创建相关的资源，包括警报、用于调用函数的 ONS 主题。模板 2 的部署与 Terraform Template-1 的部署类似。

过程

步骤 1 登录 OCI 门户。

区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**开发人员服务 (Developer Service)** > **资源管理器 (Resource Manager)** > **堆栈 (Stack)** > **创建堆栈 (Create Stack)**.

选择目标文件夹中的 *Terraform template template2.zip* 作为 Terraform 配置的源。

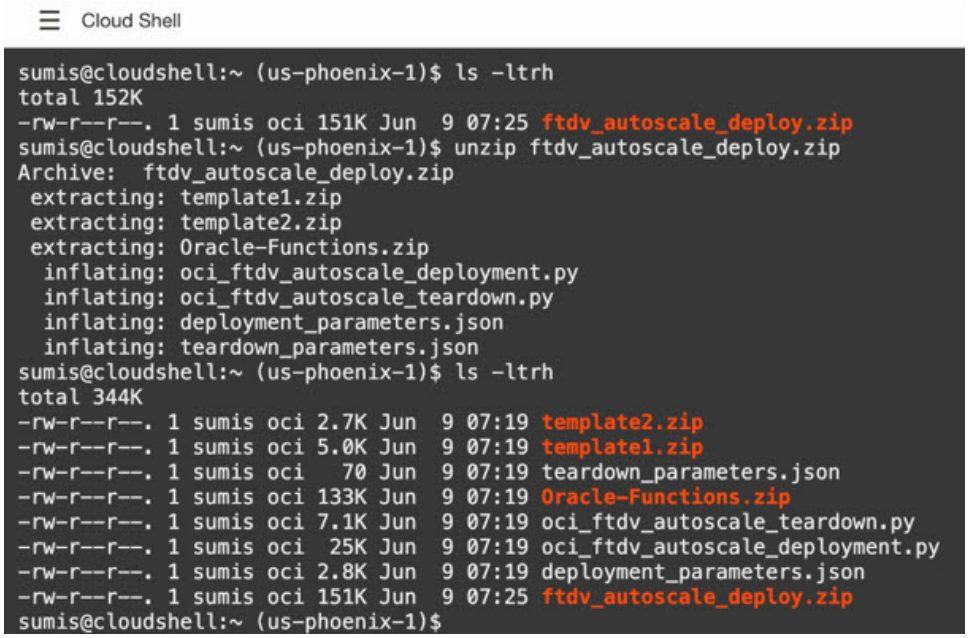
步骤 3 在下一步中，点击**Terraform 操作 (Terraform Actions)** > **应用 (Apply)**。

使用 Cloud Shell 部署

为避免部署开销，您可以通过调用简单的端到端部署脚本来部署 AutoScale 解决方案（Terraform template1、template2 和 oracle 功能）。

过程

步骤 1 将目标文件夹中的 *ftdv_autoscale_deploy.zip* 文件上传到 Cloud Shell 并解压缩文件。



步骤 2 在执行 *python3 make.py* 构建命令之前，请确保您已更新 `deployment_parameters.json` 中的输入参数。

步骤 3 要启动 Autoscale 解决方案部署，请在 Cloud Shell 上运行 `python3 oci_ftdv_autoscale_deployment.py` 命令。

完成解决方案部署大约需要 10-15 分钟。

如果在解决方案部署过程中出现任何错误，则错误日志会被保存。

验证部署

验证是否已部署所有资源，并且 Oracle 功能是否已与警报和事件连接。默认情况下，实例池的最小和最大实例数为零。您可以使用所需的最小和最大数量在 OCI UI 中编辑实例池。这将触发新的 threat defense virtual 实例。

我们建议您仅启动一个实例并检查其工作流程，并验证其行为以确保符合预期。完成验证后，您可以部署 threat defense virtual 的实际要求。

注释 将 threat defense virtual 实例的最小数量指定为**受扩展保护 (Scale-In protected)**，以避免被 OCI 扩展策略删除。

升级

升级 Autoscale 堆栈

此版本不支持升级。应重新部署堆栈。

升级 Threat Defense Virtual VM

此版本不支持升级 threat defense virtual VM。应使用所需的 threat defense virtual 映像来重新部署堆栈。

实例池

1. 要更改实例池中的最小和最大实例数，请执行以下操作：

   点击**开发人员服务 (Developer Services)** > **功能 (Function)** > **应用名称 (Application Name)** > （**通过 Terraform Template-1 创建**） **配置 (Configuration)**。

   分别更改 min_instance_count 和 max_instance_count。

2. 删除/终止实例不等于内向扩展。如果实例池中的任何实例因外部操作而并非内向扩展操作而被删除/终止，则实例池会自动启动新实例进行恢复。

3. Max_instance _count 定义外向扩展操作的阈值限制，但可以通过 UI 更改实例池的实例计数来超过此限制。确保 UI 中的实例计数小于在 OCI 应用中设置的 max_instance_count。否则，请相应地增大阈值。

4. 直接从应用减少实例池中的实例计数不会执行以编程方式设置的清理操作。由于这些后端不会从两个负载均衡器中耗尽和删除，如果 threat defense virtual 有许可证，它将丢失。

5. 由于某些原因，如果 threat defense virtual 实例在一段时间内运行状况不佳、无响应且无法通过 SSH 访问，则实例会被强制从实例池中删除，任何许可证都可能丢失。

Oracle 功能

- Oracle 功能实际上就是 Docker 映像。这些映像会别保存到 OCI 容器注册表的根目录中。这些映像不应被删除，否则也会删除在 Autoscale 解决方案中使用的功能。
- 通过 Terraform Template-1 创建的 OCI 应用包含 Oracle 功能正常工作所需的关键环境变量。除非强制要求，否则不应更改这些环境变量的值和格式。所做的任何更改只会反映在新实例中。

负载均衡器后端集

在 OCI 中，仅支持使用配置为 threat defense virtual 中的管理接口的主接口来连接到实例池的负载均衡器。因此，内部接口会连接到内部负载均衡器的后端集；外部接口会连接到外部负载均衡器的后端集。这些 IP 不会自动添加到后端集或从后端集中删除。我们的 Auto Scale 解决方案会以编程方式处理这两个任务。但在进行任何外部操作、维护或故障排除时，可能会有需要手动完成此操作的情况。

根据要求，可以使用侦听程序和后端集在负载均衡器上打开更多端口。即将启用的实例 IP 会被自动添加到后端集中，但应手动添加现有实例 IP。

在负载均衡器中添加侦听程序

要在负载均衡器中添加某个端口作为侦听程序，请转至 **OCI** > **网络 (Networking)** > **负载均衡器 (Load Balancer)** > **侦听程序 (Listener)** > **创建侦听程序 (Create Listener)**。

将后端注册到后端集

要将 threat defense virtual 实例注册到负载均衡器，应将 threat defense virtual 实例外部接口 IP 配置为外部负载均衡器后端集中的后端。内部接口 IP 应配置为内部负载均衡器后端集中的后端。确保您正在使用的端口已被添加到侦听程序中。

从 OCI 中删除 Autoscale 配置

可以使用 OCI 中的资源管理器以相同的方式删除使用 Terraform 部署的堆栈。删除堆栈会删除其创建的所有资源，并且与这些资源关联的所有信息都会被永久删除。

注释 在堆栈删除的情况下，建议将实例池中的最小实例数设置为 0，然后等待实例终止。这样将有助于删除所有实例，并且不会留下任何残留。

您可以执行手动删除或使用 使用 Cloud Shell 来删除 Autoscale 。

手动删除

删除端到端 Auto Scale 解决方案包括三个步骤：删除 Terraform Template-2 堆栈、删除 Oracle 功能，然后是删除 Terraform Template-1 堆栈 。

删除 Terraform Template-2 堆栈

要删除 Autoscale 配置，您必须先删除 Terraform Template-2 堆栈。

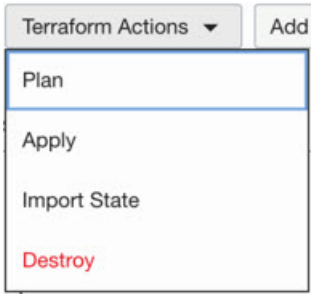
过程

步骤 1 登录 OCI 门户。

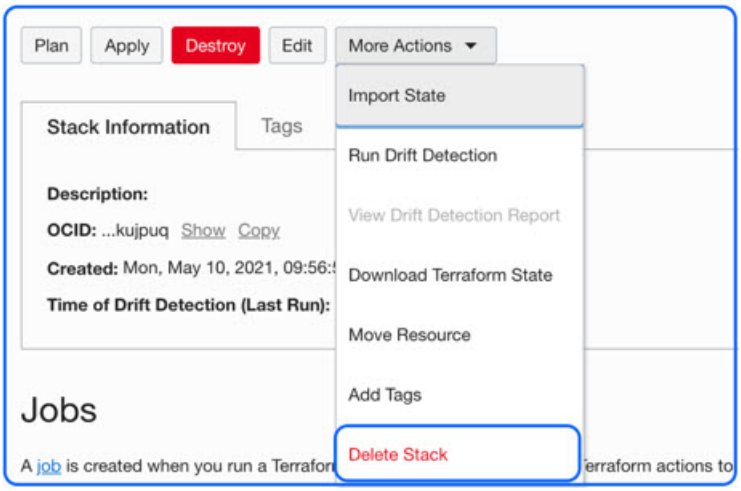
区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**开发人员服务 (Developer Services)** > **资源管理器 (Resource Manager)** > **堆栈 (Stack)**。

步骤 3 选择 Terraform Template-2 创建的堆栈，然后选择**Terraform 操作 (Terraform Actions)** 下拉菜单中的**销毁 (Destroy)**，如图所示。



将创建销毁作业，逐个删除资源需要一些时间。您可以在销毁作业完成后删除堆栈。如下图所示：



步骤 4 继续删除 Oracle 功能。

删除 Oracle 功能

Oracle 功能部署不是 Terraform 模板堆栈部署的一部分，它要使用 Cloud Shell 单独上传。因此，Terraform 堆栈删除也不支持其删除。您必须删除通过 Terraform Template-1 创建的 OCI 应用内的所有 Oracle 函数。

过程

步骤 1 登录 OCI 门户。

区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**开发人员服务 (Developer Services)** > **功能 (Functions)**。选择在模板 1 堆栈中创建的应用名称。

步骤 3 在此应用中，访问每个函数并将其删除。

删除 Terraform Template-1 堆栈

注释 只有在删除所有 Oracle 功能之后，才能成功删除模板 1 堆栈。

与 Terraform Template-2 删除相同。

过程

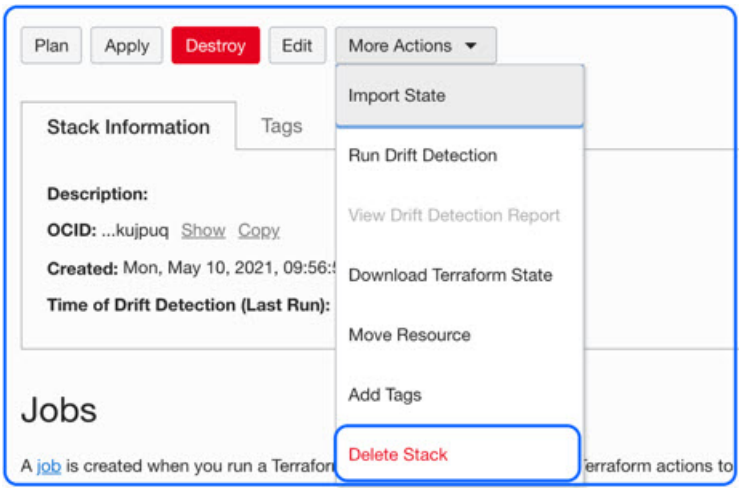
步骤 1 登录 OCI 门户。

区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**开发人员服务 (Developer Services)** > **资源管理器 (Resource Manager)** > **堆栈 (Stack)**。

步骤 3 选择 Terraform Template-2 创建的堆栈，然后点击 **Terraform 操作 (Terraform Actions)** 下拉菜单中的**销毁 (Destroy)**。系统将创建销毁作业，逐个删除资源需要一些时间。

步骤 4 销毁作业完成后，您可以从**更多操作 (More Actions)** 下拉菜单中删除堆栈，如下图所示。



成功删除 Terraform Template-1 堆栈后，您必须验证是否所有资源均已删除，并且没有任何类型的残留。

使用 Cloud Shell 来删除 Autoscale

用户可以在 Cloud Shell 中执行 `python3 oci_ftdv_autoscale_teardown.py` 命令，一般使用脚本删除堆栈和 Oracle 功能。如果堆栈是手动部署的，请更新 stack1 和 stack2 的堆栈 ID，然后更新 *teardown_parameters.json* 文件中的应用 ID。

使用 SSH 连接到 Threat Defense Virtual实例

要从 Unix 风格的系统连接到 threat defense virtual 实例，请使用 SSH 登录实例。

过程

步骤 1 使用以下命令设置文件权限，以便只有您可以读取文件：

```
$ chmod 400 <private_key>
```

其中：

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

步骤 2 使用以下 SSH 命令访问实例：

```
$ ssh  -i <private_key> <username>@<public-ip-address>
```

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

<username> 是 threat defense virtual 实例的用户名。

<public-ip-address> 是您从控制台检索的实例 IP 地址。

使用 OpenSSH 连接到 Threat Defense Virtual实例

要从 Windows 系统连接到 threat defense virtual 实例，请使用 OpenSSH 登录实例。

过程

步骤 1 如果这是您首次使用此密钥对，则必须设置文件权限，以便只有您能读取文件。

执行以下操作：

a) 在 Windows 资源管理器中，导航至私钥文件，右键点击该文件，然后点击**属性 (Properties)**。
b) 在**安全 (Security)** 选项卡上，点击**高级 (Advanced)**。
c) 确保**所有者 (Owner)** 是您的用户帐户。
d) 点击**禁用继承 (Disable Inheritance)**，然后选择**将此对象的继承权限转换为显式权限 (Convert inherited permissions into explicit permissions on this object)**。
e) 选择不是您的用户帐户的每个权限条目，然后点击**删除 (Remove)**。
f) 确保您的用户帐户的访问权限为**完全控制 (Full control)**。
g) 保存更改。

步骤 2 要连接到实例，请打开 Windows PowerShell 并运行以下命令：

```
$ ssh  -i <private_key> <username>@<public-ip-address>
```

其中：

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

<username> 是 threat defense virtual 实例的用户名。

<public-ip-address> 是您从控制台检索的实例 IP 地址。

使用 PuTTY 连接到 Threat Defense Virtual实例

要使用 PuTTY 从 Windows 系统连接到 threat defense virtual 实例，请执行以下操作：

过程

步骤 1 打开 PuTTY。

步骤 2 在**类别 (Category)** 窗格中，选择**会话 (Session)** 并输入以下内容：

- **主机名（或 IP 地址）：**

  <username>@<public-ip-address>

  其中：

  <username> 是 threat defense virtual 实例的用户名。

  <public-ip-address> 是您从控制台检索的实例公共 IP 地址。

- **端口：** 22
- **连接类型：** SSH

步骤 3 在**类别 (Category)** 窗格中，展开**窗口 (Window)**，然后选择**转换 (Translation)**。

步骤 4 在**远程字符集 (Remote character set)** 下拉列表中，选择 **UTF-8**。

基于 Linux 的实例的默认区域设置为 UTF-8，这样会将 PuTTY 配置为使用相同的区域设置。

步骤 5 在**类别 (Category)** 窗格中，依次展开**连接 (Connection)** 和 **SSH**，然后点击**身份验证 (Auth)**。

步骤 6 点击**浏览 (Browse)**，然后选择您的私钥。

步骤 7 点击**打开 (Open)** 以启动会话。

如果这是第一次连接到实例，您可能会看到一条消息，表明服务器的主机密钥未缓存在注册表中。点击**是 (Yes)** 以继续连接。

IPv6 故障排除

问题 SSH - 使用 IPv6 的 Firewall Threat Defense Virtual 不工作

- 解决方法 确保已添加通过互联网网关进行 IPv6 公共访问的路由。
- 解决方法 Firewall Threat Defense Virtual 管理配置中存在启用 IPv6。
- 解决方法 验证已将 IPv6 相关访问列表添加到已部署的 Firewall Threat Defense Virtual。
- 解决方法 验证是否使用“ipv6 address dhcp default”在管理接口上配置 IPv6。如果仅使用“ipv6 address dhcp”，则单独添加以下路由“ipv6 route management ::/0<IPv6_Gateway_address>”。
- 解决方法 验证是否允许正确的 ssh 入口。使用以下命令为所有“ssh ::/0 management”设置 ssh access allow。

问题 无法将 IPv6 地址分配给现有子网。

- 解决方法 验证子网所属的 VCN 是否已启用 IPv6。
- 解决方法 确保使用的是正确的 IPv6 CIDR。
- 解决方法 子网只能包含“/64”IPv6 CIDR 前缀。

问题 东西向流量不起作用。

- 解决方法 验证是否已正确添加以下路由。

  解决方法 ipv6 route <interface_name> <interface_subnet_CIDR> <ipv6_virtual_router_ip>

  解决方法 示例：ipv6 route inside 2603:c020:5:5800::/56 fe80::200:17ff:fe96:921b

- 解决方法 确保使用的是正确的 IPv6 CIDR。
- 解决方法 确保是否为 IPv6 配置了正确的访问列表。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。